

COPYING PREVENTION DEVICE AND METHOD**Publication number:** JP2000076141**Publication date:** 2000-03-14**Inventor:** MORIFUJI HAJIME; YOSHIURA YUTAKA**Applicant:** HITACHI LTD**Classification:****- international:** **G06F12/14; G06F21/24; G11B20/00; G11B20/10; G06F1/00; G06F12/14; G06F21/00; G11B20/00; G11B20/10; G06F1/00; (IPC1-7): G06F12/14****- European:** G11B20/00P**Application number:** JP19990091260 19990331**Priority number(s):** EP19980307028 19980902**Also published as:**

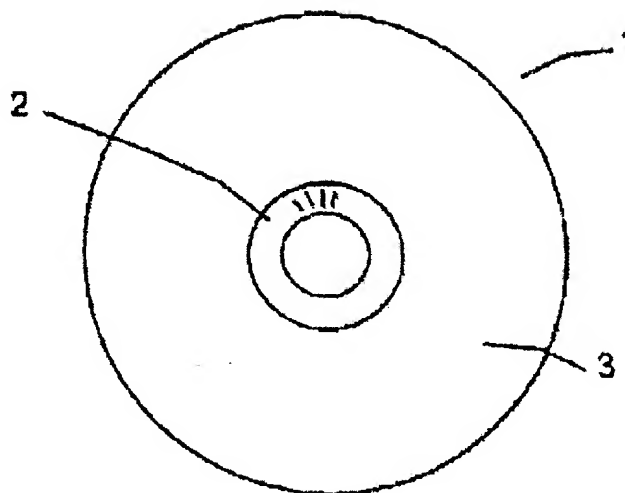
EP0984346 (A1)

US6782190 (B1)

Report a data error here**Abstract of JP2000076141**

PROBLEM TO BE SOLVED: To protect digital data on a data storage medium from unauthorized copying even when copying prevention information inside the data is forged.

SOLUTION: Copying protective device and method to be used in a digital data recorder like a DVD-RAM include the use of a DVD disk 1 provided with a unique serial number stored in the read-only part 2 of a disk for data recording. The serial numbers of the respective disks are digitally signed together with other copying control information. The digital signature is verified in a DVD player/recorder and whether or not the disk to be reproduced is an original disk or a proper copy is checked. When it is not either one, the reproduction recording of the data of the disk are blocked. A copying generation management system is executed by the use of the copying control information as well.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-76141
(P2000-76141A)

(43)公開日 平成12年3月14日(2000.3.14)

(51)IntCl⁷

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

テマコード*(参考)

3 2 0 E

審査請求 未請求 請求項の数23 O L (全 13 頁)

(21)出願番号 特願平11-91260

(22)出願日 平成11年3月31日(1999.3.31)

(31)優先権主張番号 9 8 3 0 7 0 2 8 . 5

(32)優先日 平成10年9月2日(1998.9.2)

(33)優先権主張国 ヨーロッパ特許庁 (E P)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 森藤 元

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72)発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74)代理人 100087170

弁理士 富田 和子

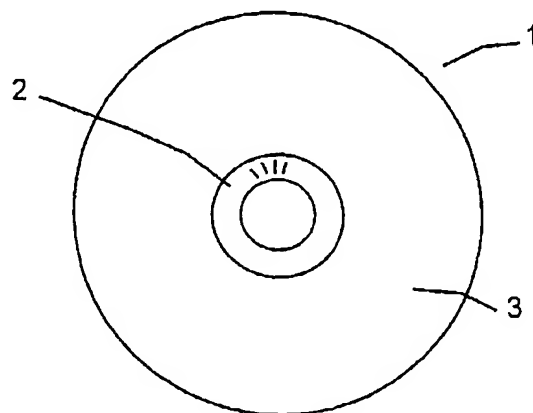
(54)【発明の名称】 コピー防止装置および方法

(57)【要約】

【課題】データ記憶媒体上のデジタルデータは、データ内のコピー防止情報が偽造されたものであっても、不正なコピーから保護する。

【解決手段】データ記録用のディスクの読み出し専用部分2に記憶された一意なシリアル番号を有するDVDディスク1を用いることを含む、DVD-RAMのようなデジタルデータレコーダで使用するコピー保護装置および方法である。各ディスクのシリアル番号は他のコピー制御情報とともにデジタル的に署名される。このデジタル署名はDVDプレーヤ/レコーダ13、30にて検証され、再生しようとしているディスクがオリジナルディスクかあるいは正当なコピーかをチェックする。いずれでもなければ、そのディスクのデータの再生および記録が阻止される。コピー制御情報の使用によっても、コピー生成管理システムを実施することができる。

図1



【特許請求の範囲】

【請求項1】媒体識別子を有する記憶媒体上に記憶されたデータを処理する装置であって、前記媒体識別子と、前記媒体上に記憶された媒体識別子の検証情報との関係に依存した記憶データの処理を制御する手段を有する装置。

【請求項2】請求項1記載の装置であって、前記媒体識別子は前記媒体の読み出し専用部分に記憶される装置。

【請求項3】請求項1または2記載の装置であって、前記媒体識別子は、第1の媒体識別子を有し、前記検証情報は第2の媒体識別子を有する装置。

【請求項4】請求項3記載の装置であって、制御手段は前記第1および第2の媒体識別子の比較に応じて動作する装置。

【請求項5】請求項4記載の装置であって、前記制御手段は、前記第1および第2の媒体識別子が異なる場合、データの再生を阻止する装置。

【請求項6】請求項4または5記載の装置であって、前記制御手段は、前記第1および第2の媒体識別子が異なる場合、データの記録を阻止する装置。

【請求項7】先行する任意の請求項に記載の装置であって、さらに、前記検証情報を認証するための手段を有する装置。

【請求項8】請求項7記載の装置であって、前記検証情報はデジタル署名され、前記認証手段は、このデジタル署名を検証する手段を有する装置。

【請求項9】先行する任意の請求項に記載の装置であって、さらに、媒体からのデータの記録を制御する手段を有する装置。

【請求項10】請求項9記載の装置であって、前記記録制御手段は、媒体上に記憶されたコピー管理データに応じて動作する装置。

【請求項11】請求項10記載の装置であって、前記コピー管理データは、媒体が自由にコピーできること、1回だけコピーできること、またはコピーできないことを指定する装置。

【請求項12】請求項10または11記載の装置であって、前記コピー管理データはデジタル的に署名される装置。

【請求項13】先行する任意の請求項に記載の装置であって、DVDプレーヤを構成する装置。

【請求項14】請求項13記載の装置であって、前記媒体はDVDディスクからなる装置。

【請求項15】媒体識別子およびこの識別子の検証情報が記憶された記憶媒体上に記憶されたデータを処理する方法であって、前記媒体上に記憶された前記媒体識別子と媒体識別子の検証情報との関係に依存して前記記憶データの処理を制御することを含む方法。

【請求項16】媒体識別子を有するデータ記憶媒体上にデータを記録する記録装置であって、前記媒体識別子の

検証情報を生成する手段を有し、前記検証情報は前記媒体上に記憶される装置。

【請求項17】請求項16記載の装置であって、前記検証情報をデジタル的に署名する手段を有する装置。

【請求項18】請求項16または17記載の装置であって、前記検証情報は媒体識別子を含む装置。

【請求項19】請求項16から18のいずれか1つに記載の装置であって、そこからデータが記録されようとしている記録元の媒体上に記憶されたコピー管理データに応じて、媒体上への記録を制御する手段を有する装置。

【請求項20】媒体識別子を有するデータ記憶媒体上へデータを記録する方法であって、前記媒体上に記憶されるべき媒体識別子の検証情報を生成することを含む方法。

【請求項21】請求項20記載の方法であって、前記媒体の読み出し専用部分から前記媒体識別子を読み出すことを含む方法。

【請求項22】請求項20または21記載の方法であって、デジタル署名を用いて前記検証情報を保護することを含む方法。

【請求項23】媒体上に記憶された媒体識別子およびこの識別子の検証情報を有するデータ記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コピー防止に関し、特に（但し、排他的にはなく）、データ記憶媒体上のデジタルデータを不正な(unauthorised)コピーから保護するための装置および方法に関する。

【0002】

【従来の技術】オーディオCDやCD-ROMのようなデジタル媒体によれば、それらに記憶されたデジタルデータを完全に複製(reproduction)することができるが、従来、これらの媒体は通常読み取り専用であるため、侵害の可能性のある者は高品質のコピーを作製するためには記録専門家およびCDプレス機器を必要とすることから、不正な複製を取り締まる問題はある程度緩和された。

【0003】しかし、広く利用される低コストのレコーダを作製することを目的とした、CD-R（ライトワンズ）やCD-RW（書き換え可能）を含む記録可能デジタル記憶技術、並びにデジタル汎用ディスク(DVD: Digital Versatile Disk)技術の消費者市場への導入に伴って、大規模な海賊行為を防止するために高度なコピー防止システムの必要性が増大してきた。DVD-RAMレコーダとして知られているDVDレコーダは、究極的には、コンピュータハードディスクおよびビデオカセットレコーダを含む、現在利用可能な種々の異なる形式の記憶装置にとって代わると予想される。

【0004】DVD技術の原理は、市販の日立製作所製GF-1000シリーズのようなDVD-RAMについ

て十分に確立されている。DVD原理の詳細情報については、McGraw-Hill社から出版されたJim Taylor著”DVD Demystified”を参照されたい。

【0005】何らかのコピー管理(copy control)なしには、DVDディスクやCD-ROMで頒布される映画、オーディオ記録および他のデジタルコンテンツは、記録可能なDVD-RAMのようなデジタルデータ記憶媒体に対してDVD-RAMや他のデジタルレコーダにより容易に記録することが可能であり、このデジタル記録媒体から、当該データをコピー品質の劣化なしに他のDVDディスクに対して多数回コピーすることができる。

【0006】不正なコピーを阻止するために、消費者に販売されている装置にはコピー防止機構が内蔵されている。例えば、Jim Taylor著”DVD Demystified”の第128頁に記載されているように、DVDディスクのデータセクタ内にコピー管理信号を埋め込むことができる。このような埋め込み情報を用いるコピー管理の可能な方法は、デジタルコンテンツの提供者がそのデータに”ネバーコピー(Never-Copy)”フラグを埋め込んで、例えばDVD-ROMディスクのような読み出し専用媒体で、映画や他のデジタルコンテンツを供給するものである。DVDプレーヤ/レコーダはこのフラグの存在をチェックし、もしフラグがある場合にそのディスクをコピーしようとする、記録回路は記録を阻止する。しかし、この種のコピー防止策は、コンピュータ用周辺機器としてのDVD-ROM/RAMデバイスを用いることにより回避することができる。これにより、記録可能ディスク上に、コピー防止情報を含めて、オリジナルディスクからデータをビット単位に記録することができる。

【0007】このようなコピー防止法の回避を防止するために、DVDプレーヤには、ROMディスクと異なり、記録可能なディスク上にネバーコピーフラグがあるか否かをチェックするよう設計されたものがある。このような記録可能なディスク上のフラグの存在は、そのディスクがオリジナルのROMディスクを不正にコピーしたものであることを示し、その結果、そのディスク上のデータの再生が阻止される。他方、ROMディスクが使用されていることをそのプレーヤが検知した場合には、そのディスク上のデータを再生する。

【0008】

【発明が解決しようとする課題】しかし、ディスクをコピーするコンピュータユーザはネバーコピーフラグを含めたデータのすべてをビット単位にコピーするという前提の下で、この方法は機能する。コピー管理情報がオリジナルROMディスク上のどこに位置しているかを認識し、または突き止めて、このオリジナルディスクを記録可能なディスク上にコピーする際に、当該情報を変更または上書きすることのできるコンピュータユーザによれば、上記方法は依然容易に回避されうる。

【0009】上記防止法の他の問題は、それに柔軟性が

なく、コピーが許可される程度を管理するコピー生成管理システム(copy generation management system: CGMS)を設ける方法が存在しないことである。

【0010】例えば、オリジナルのデータ記憶媒体の内容をバックアップ媒体にコピー可能としながら、そのバックアップ媒体から更に別のコピーの生成は阻止するような方法が存在しない。

【0011】本発明は、このような問題に対処することを目的とする。

【0012】

【課題を解決するための手段】本発明によれば、媒体識別子を有する記憶媒体上に記憶されたデータを処理する装置が提供される。この装置は、媒体上に記憶された媒体識別子と、媒体識別子の検証情報との関係に依存した記憶データの処理を制御する手段を有する。

【0013】前記媒体識別子は第1の媒体識別子であり、前記検証情報は第2の媒体識別子からなり、前記装置は、第1および第2の媒体識別子が異なる場合に、再生または記録を阻止することができる。

【0014】オリジナルディスクの場合、第2の媒体識別子は第1の媒体識別子のコピーであってもよい。

【0015】本装置は、検証情報を認証する手段を有してもよい。検証情報は、例えばデジタル署名され、認証手段はデジタル署名を検証する手段を有する。

【0016】本発明はさらに、媒体上に記憶された媒体識別子および識別子の検証情報を有する記憶媒体に記憶されたデータを処理する方法を提供する。この方法は、媒体識別子と検証情報との関係に依存して記憶データの処理を制御することを含む。

【0017】本発明は、媒体識別子を有するデータ記憶媒体上にデータを記録するための記録装置も提供する。この装置は、媒体上に記憶されるべき、媒体識別子の検証情報を生成する手段を有する。

【0018】記録装置は、データがそこから記録されている記録元の媒体上に記憶されたコピー管理データに応じて、媒体上への記録を制御する手段を有してもよい。

【0019】本発明は、さらに、媒体識別子を有するデータ記憶媒体上へデータを記録する方法を提供する。この方法は、媒体上に記憶されるべき媒体識別子の検証情報を生成することを含む。

【0020】本発明によれば、さらに、媒体上に記憶された媒体識別子および媒体識別子の検証情報を有するデータ記憶媒体が提供される。

【0021】本発明によれば、有利なことに、データ記憶媒体上のデジタルデータは、データ内のコピー防止情報が偽造されたものであっても、不正なコピーから保護することができる。また、この防止法は、バックアップコピーのような合法的なコピーの生成を可能とする。

【0022】

【発明の実施の形態】以下、本発明の実施形態を、添付

の図面を参照しながら例示説明する。

【0023】図1において、本発明によるDVDディスク1は、識別子領域2とデータ領域3とを有する。識別子領域はディスクの読み出し専用部分に位置するので、ディスクの製造者のみがディスク1の製造時にこの領域に情報を書き込むことができる。例えば、識別子領域2はDVDディスクのバーストカット領域(burst cutting area)でありうる。さらなる詳細はJim Taylor著”DVD Demystified”の第125～126頁を参照されたい。

【0024】図2において、まず未記録(ブランク)DVDディスク4が媒体製造器5により従来の製造工程により製造される。DVD媒体の製造工程はCD-RやCD-RWディスクを製造するのに利用される工程と同様である。例えば、コンピュータ稼働シリアル番号生成ソフトウェアである媒体識別子発生器6は、例えばシリアル番号である固有の(一意な)識別子を生成する。この固有の識別子は、媒体識別子プリンタ7によりブランクDVDディスク4のバーストカット領域2に書き込まれ、これにより、データ書き込みが可能なブランクDVDディスク1が製造される。媒体識別子プリンタ7は、例えば、レーザ構成で、バーストカット領域2にストライプ状の一連のバーコードを刻むことによりシリアル番号を表す。實際上、この識別子は固有であるに越したことはないが、このことは必須ではない。重要なのは、広範なコピーを阻止するために、消費者が同一の識別子番号を持ったディスクを容易に入手できるという状況が殆ど起こりそうにないということである。

【0025】DVDディスク1のデータ領域3へのアクセス可能性は、関与するディスクの型に依存する。DVD-ROMディスクの場合、この領域は読み出し専用である。DVD-ROMディスクは、Jim Taylor著”DVD Demystified”の第121～123頁に記載されているように、マスターコピーからそれを刻印(スタンプ)することにより生成することができる。これは、大量のディスクを製造する場合に最も費用効率のよい工程である。DVD-ROMディスクの他の製造技術によれば、個々のディスクに対して固有のデータを内容させることができる。

【0026】DVD-R(ライトワンス)ディスクの場合、製造者は、識別子領域2内に例えば固有のシリアル番号を有するブランクディスクを製造する。但し、データ領域3は、コンテンツ供給者により、従来のデータ書き込み装置を用いて、一度だけ書き込みを行うことができる。一旦、コンテンツ供給者がディスクにデータを書き込むと、そのディスクは実質的にはDVD-ROMと同様に機能し、消費者が再書き込みを行うことはできない。

【0027】また、ディスク1はDVD-RAM(再書き込み可能)ディスクでありうる。これは、典型的には、消費者が記録および再記録できるブランクディスク

として頒布される。

【0028】消費者へ頒布するための記録済みディスクの製造の背景にある原理については、DVD-Rディスク1を参照して以下に説明する。このディスクは、例えば図2に示した製造構成で製造される。その結果、このディスク製造者からブランクディスクをコンテンツ供給者が受け取る。各ブランクディスクには、製造段階で、固有のディスク識別子、例えばシリアル番号が識別子領域2に書き込まれている。コンテンツ供給者は、ついで、映画、オーディオデータ、または他のデジタルコンテンツ(ここでは総称してデータと呼ぶ)、およびディスク1の他の関連情報(図3に示した記録装置8を参照して説明する)を記録することができる。

【0029】コンテンツ供給者により使用されるべき記録装置8の一例は、DVDディスク1の読み出し専用部分2からディスク識別子を読み出す読み出し装置9と、コピー管理情報(CCI)生成器10と、この生成されたコピー管理情報をデータアーカイブ12からのデータとともにディスク1上に記録する記録モジュール11とを有する。

【0030】記録装置8の動作を示す図4において、ステップs1で、読み出し装置9が記録中のディスク1からディスク識別子を読み出し、この識別子をCCI生成器10へ渡す。CCI生成器10は、このディスク識別子の検証情報を、コピー管理情報として生成する(s2)。ステップs3では、記録モジュール11がデータアーカイブ12からデータを読み出し、これを、CCI生成器10からのコピー管理情報とともにディスク1上に記録する(s4)。こうして得られた記録済みディスク1はここではオリジナルディスクと呼ぶ。

【0031】図5において、本発明によるDVDプレーヤ13は、読み出し装置14と、CCI検証モジュール15と、再生装置16とを有する。プレーヤ13の動作を示す図6において、ステップs5では、読み出し装置14が再生しようとしているディスク1からデータ、コピー管理情報およびディスク識別子を読み出し、この情報をCCI検証モジュール15へ送る。ステップs6では、検証モジュール15がコピー管理情報を検証しようとする。すなわち、コピー管理情報およびディスク識別子から、再生しようとしているディスクがオリジナルディスクか許可されたコピーかあるいは不正なコピーかを判定する。検証結果に問題がなければ、制御はステップs7へ進み、再生装置16がデータを再生する。検証結果に問題があれば、制御はステップs8へ進み、再生が阻止される。なぜなら、検証処理が失敗したことは、読み出そうとしているディスクが不正コピーであることを意味するものと理解されるからである。

【0032】ここで説明する本発明のすべての例において、読み出しモジュール11、読み出し装置9、14および再生装置16のような、DVDディスクに対してデ

ータを読み書きするに要する装置は、日立製作所製GF-1000シリーズのような市販のDVDプレーヤ/レコーダにおいて現在使用されているような従来の回路で実施することができる。CCI生成器10およびCCI検証器15のような、本発明を実施するために必要なブロックの機能は、従来のマイクロプロセッサを基本として回路上でソフトウェアによって実施することができる。

【0033】ディスク1上に記録できるコピー管理情報の一例は、記録装置8内の読み出し装置9で読み出されるオリジナルディスク識別子の単なるコピーである。図7において、ステップs9では、読み出し装置9がオリジナルディスクからディスク識別子Sdを読み出し、ステップs10で、Sdをコピー管理情報として保存する。ステップs11では、記録モジュール11がデータアーカイブ12からデータを読み出して、このデータおよびSdをディスク1のデータ領域3へ記録する(s12)。ステップs13では、再生しようとしているディスクのディスク識別子であるSpを、プレーヤ13内の読み出し装置14がディスク1のバーストカット領域2から読み出し、これをCCI検証器15へ送る。読み出し装置14はまた、コピー管理情報すなわちSdをディスク1のデータ領域3から読み出す。ステップs14では、CCI検証器15が実際のディスク識別子Spをオリジナルディスク識別子Sdのコピーと比較する。もしオリジナルディスクがコピーされたものでなければ、2つの識別子、例えば、各ディスクのシリアル番号が同一となり、そのディスクが再生可能であることを示す信号が再生装置16へ送られる(s15)。一方、オリジナルディスクがコピーされたのであれば、すなわち、オリジナルディスク上のすべてのデータが新たなディスクへ転送されたのであれば、新たなディスクのバーストカット領域2内のディスク識別子Spは、新たなディスクのデータ領域3にコピーされたオリジナルディスク識別子Sdと異なることになる。この場合、そのディスクは不正にコピーされたものであり、再生できないという信号が再生装置16へ送られる(s16)。

【0034】コピー管理情報としてオリジナルディスク識別子のコピーを用いることは、前述したネバーコピーフラグの使用と同様の再生コピー管理の一形式を提供する。したがって、オリジナルディスクのコピーの作成自体は阻止されないが、この例によるDVDプレーヤは当該コピー上のデータを再生しない。しかも、コピーされたディスクから第2世代のコピーを生成すること自体は、ステップs14～s16で説明したようなプレーヤ13と同じ検証チェックを行うことにより阻止される。これが機能するのは、SpがSdと異なる場合のコピーを、第1世代のコピーであると記録装置が認識して、更なる記録を阻止することができるからである。

【0035】上述のコピー管理方法によるコピー防止を

消費者が回避することを禁止するために、コピー管理情報自体はアクセスや変更から保護される必要があると考えられる。

【0036】適切な形式の保護の一例は、公開鍵暗号システムを基礎とすることができるデジタル署名を使用するものである。デジタル署名の形成方法は周知であり、デジタル署名ソフトウェアは、例えば、米国カリフォルニア州にあるRSAデータセキュリティ社から市販されており、これは周知のRSA公開キーアルゴリズムを用いるものである。公開鍵システムの原理およびそのデジタル署名への使用について以下に説明する。より詳細な説明は、Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc. 1996, ISBN 0-471-11709-9を参照されたい。

【0037】公開鍵暗号は、キー対(key pairs)として知られる、相互に逆方向の数学的演算(mutually inverse mathematical operations)の非対称対の使用に基づくものである。

【0038】例えば、Eが公開鍵アルゴリズムであるとすると、表記 $E_k(m)$ はキーKを用いたメッセージmの暗号化を意味する。

【0039】もし、Kと K^{-1} がEのキー対であるならば、 $E_k(E_{k^{-1}}(m)) = m$ となる。よって、キー K^{-1} (ここでは秘密鍵という)で暗号化されたメッセージは、キーK(ここでは公開鍵という)を適用することにより解読することができる。公開鍵暗号は、キーのビット長が十分大きい(例えば512ビット以上)とき、現状では、キー対の一方から他方を算出するには計算上不可能であるという事実に基づくものである。

【0040】デジタル署名は、公開鍵アルゴリズムおよび一方方向ハッシュ関数に基づくことができる。ハッシュ関数は、可変長入力列を受けてこれを、ハッシュ値として知られる一般により小さい出力列に変換する任意の関数である。一方方向ハッシュ関数とは、メッセージmが与えられたとき、ハッシュ値 $c = H(m)$ を計算することが容易であるが、与えられたハッシュ値cを基にmを算出することが困難であるような関数である。Hの出力ビット長が十分大きい(例えば128ビット以上)場合、一般にcからmを求めることは計算上不可能である。参考としてBruce Schneier, "Applied Cryptography", pp. 29-31, pp. 38-39, D.W. Davies, W.L. Price, "The Application of Digital Signatures Based on Public-Key Cryptosystems", Proceedings of the Fifth International Computer Communications Conference, October 1980, pp. 525-530、およびNational Physical Laboratory Report DNACS 39/80, December 1980を参照されたい。

【0041】デジタル署名の使用を可能とする方法を以下に説明する。

【0042】例えば、XがYへメッセージを送りたいとする。メッセージの内容は秘密ではないが、Yはそのメ

ッセージがXから発せられたものであること、および、それが第三者により改竄されていないことを確信したい。したがって、Xは公開鍵アルゴリズムEのキー対Kおよび K^{-1} を生成する。Xは秘密鍵 K^{-1} を保持し、キーKを公衆に公開する。そこで、Xは、メッセージmを作成し、これに対して次のようにしてデジタル的に署名する。

【0043】1. $c = H(m)$ を計算する。ここに、Hは既知のハッシュ関数である。

【0044】2. 秘密鍵 K^{-1} を用いてEによりcを暗号化する。

【0045】すなわち、デジタル署名 $= E_{K^{-1}}(c)$ デジタル署名は、ここでは、 $Si g_{K^{-1}}(m)$ と表されるので、上記式は次のように書ける。

【0046】 $Si g_{K^{-1}}(m) = E_{K^{-1}}(c)$
Yがメッセージmを受け取ったとき、Yは次の手順により、Xの公開鍵Kを用いて署名を検証することができる。

【0047】1. $c' = H(m)$ を計算する。

【0048】2. キーKを用いて $E_{K^{-1}}(c)$ を復号し、c、すなわち $c = E_K(E_{K^{-1}}(c))$ を求める。

【0049】3. cと c' とを比較する。

【0050】もし、 $c = c'$ であれば、検証は成功であり、そうでなければ検証失敗である。

【0051】メッセージmに何らかの変更があった場合に検証失敗となる。なぜなら、この場合、メッセージ c' のハッシュが変わるからである。また、デジタル署名が偽造された場合にも検証は失敗となる。秘密鍵 K^{-1} にアクセスできるのはXのみであるから、公開鍵Kで検証できる正しいデジタル署名を生成できる唯一の人物はXである。

【0052】図3に戻り、オリジナルディスク識別子のコピーを用いる上記概説した簡単な場合に上記の保護形成を適用することにより、再生しようとしているディスクの正当性を検証するため、記録装置8内のCCI生成器10は、キー対K、 K^{-1} を生成するキー対生成器からの入力端を有する。DSAやRSAアルゴリズムのような特定のアルゴリズムの生成器を含むキー対生成器ソフトウェアは、広く市販されているものを入手可能であり、例えば、Java(商標)プログラミング言語で実施できる。例えばJava APIは、Java.security.KeyPairGeneratorとして知られているキー対生成クラスを内包している。オリジナルディスクのディスク識別子を表すディスク識別子Sdは、読み出し装置9によりディスク1から読み出され、秘密鍵 K^{-1} と、記録装置およびプレーヤの両方で固定の適当な方向ハッシュ関数H(x)とを用いてデジタル署名 $Si g_{K^{-1}}(Sd)$ が形成される。

【0053】適当なハッシュ関数の一例は、前述した"Applied Cryptography"のpp.442-445に記載されたSecure

Hash Algorithm (SHA)である。このアルゴリズムは、可変長入力ビット列を受けて、160ビットのハッシュを出力する。典型的には、決定されたハッシュ関数の知識は、非開示契約に基づいて記録装置/プレーヤ機器ベンダーに制限される。デジタル署名 $Si g_{K^{-1}}(Sd)$ は、公開キーKとともにディスク1上に記録される。

【0054】図5に戻り、プレーヤ13では、読み出し装置14は、再生しようとしているディスク1のデータ領域3から公開キーKおよび $Si g_{K^{-1}}(Sd)$ を読み、識別子領域2からディスク識別子Spを読む。CCI検証器15は、ハッシュ値H(Sp)を算出し、Kを用いて $Si g_{K^{-1}}(Sd)$ を解読することによりハッシュ値H(Sd)を得る。CCI検証器15は、ついで、これらの2つのハッシュ値を比較する。SdとSpが等しければ、再生しようとしているディスクはオリジナルディスクなので、ハッシュ値も同一であり、検証は成功し、再生を許可する信号が再生装置16へ送られる。SdとSpが等しくなければ、再生しようとしているディスクはオリジナルディスクのコピーなので、それらのハッシュ値は異なり、その結果、検証処理は失敗となり、これにより再生装置16に対して再生を阻止する信号が発せられる。

【0055】コンテンツ供給者は、秘密キー K^{-1} にアクセスできる唯一の者なので、オリジナルディスクのシリアル番号または他の識別子を正しく暗号化できる唯一の者である。

【0056】さらに複雑なコピーの管理を可能とするために、コピー管理情報の一部として他の情報を含めることができる。これは、例えば、コピー生成管理が可能なコピー管理フィールドである。

【0057】図8と図9は、コンテンツ供給者により使用される記録装置20の他の例の概略構成、および、記録済みコピー防止ディスクの生成に関するステップを説明するためのものである。

【0058】ステップs17では、キー対生成モジュール21が署名検証のための公開アルゴリズムのキー対を生成する。ステップs18では、読み出し装置22がディスク1の読み出し専用部分からDVDディスク1の識別子、例えば、シリアル番号を読み出す。ステップs19では、コピー管理情報(CCI)生成器23が、キー、識別子、およびコピー管理フィールド(CCF)データベース24からのコピー管理フィールドに基づいてデジタル署名を含むコピー管理情報を生成する。このコピー管理フィールドは、コピー自由(Copy-Freely)、ネバーコピー(Never-Copy)、コピーワンス(Copy-Once)、およびノーモアコピー(No-More-Copy)の4つの採りうる値のうちの1つを採ることができる。コピー管理情報を作成するための実際の情報について以下に詳述する。ステップs20では、記録モジュール25が、DVDディスク1に書かれるべきデータをデータアーカイブ26か

ら読み出し、このデータとCCI生成器23からのコピー管理情報とをDVDディスク1に書き込むことにより、コピー防止化された記録済みDVDディスクが完成する。

【0059】DVDプレーヤの概略構成および機能については、図5および図6により既に説明した。

【0060】図10は、消費者が記録可能ディスク上にデータを記録するために用いる本発明の記録装置30の構成を示す。図10および図11において、ステップs22で、入力信号処理モジュール31は、前述したようにディスクプレーヤ13からコピー管理情報および記録対象のデータを受け取り、これらをCCI検証器モジュール32およびCCI生成器33へ送る。ステップs23では、CCI検証器32がコピー管理情報を検証しようとする。CCI検証器32は、プレーヤ13内のCCI検証器15と同じ検証機能を実行する。もし、プレーヤと記録装置が単一ユニットとして実現されている場合、検証器32は同じ回路または同じソフトウェア機能により実現される。しかし、記録装置30がプレーヤ13とは別のユニットである場合、CCI検証器32は二重チェック機能として実装され、プレーヤに検証機能を与える。このプレーヤにはコピー保護機能は含まなくてよい。

【0061】この段階で検証が失敗したら(s23)、制御はステップs29へ移行し、新たなディスク上へのデータの記録は阻止される。検証が成功であれば、制御はステップs24へ進み、ここで、例えばコピーフリーフラグの存在により、データが自由にコピーできることをコピー管理フィールドが示しているか否かをCCI検証器32が判定する。もしデータが自由にコピーできるならば、制御はステップs28へ移行し、ここで、記録モジュール34がコピー管理情報およびデータを新たなディスク35へ記録する。ステップs24でもしデータが自由にコピーできないことをコピー管理情報が示していれば、制御はステップs25へ移行し、ここで、例えばコピーワンスフラグの存在により、データが1回だけコピーできることをコピー管理フィールドが示しているか否かをCCI検証器32が判定する。もし、フラグがコピーワンスフラグでなければ、ネバーコピーかノーモアコピーフラグがセットされていることになり、制御はステップs29へ進み、ここで記録が阻止される。一方、ステップs25で、コピーワンスフラグがセットされていることをコピー管理情報が示していたら、制御はステップs26へ進み、ここで、読み出し装置26が、新たなディスク35の媒体識別子をそのディスクの読み出し専用部分から読み出し、この識別子をCCI生成器33へ送る。ステップs27では、CCI生成器はコピー管理フィールドをコピーワンスからコピーノーモアに変え、記録モジュール34でディスク35に記録されるべき新たなコピー管理情報を生成する。この新たなコピ

ー管理情報の性質(nature)については後に詳述する。

【0062】オリジナルディスクに書き込まれるコピー管理情報の厳密な性質は、コンテンツ供給者が達成したい保護のレベルに依存する。例えば、供給者は、例えばそのDVDオーディオディスクの内容を全くコピー不可能としようとするかもしれない。あるいは、供給者はオリジナルのバックアップコピーを生成する能力を顧客に対して与えるが、それ以上のコピーの生成能力は与えたくないかもしれない。これらの目的を達成可能な方法については、次のような表記を用いて以下に説明する。

【0063】IDはコンテンツ供給者を識別する情報である。これは、供給者の名称、コンテンツの名称、生成日、等を含みうる。CCFは、上述したように、コピー自由、ネバーコピー、コピーワンス、ノーモアコピーの値を採りうるコピー管理フィールドを表す。AおよびA'は、供給者依存情報IDおよびCCFと一緒にグループ化するのに便利な表記として用いる。例えば、 $A = ID | CCF$ かつ $A' = ID | CCF'$ の如くである。ここに、CCF'は新たなディスク上への記録時にコピー管理フィールドの値の変化を表す。Sd, Sc, Spは、ディスクの読み出し専用部分に印刷されたディスク識別子である。したがって、これらの識別子は顧客によって変更されない。Sdは、オリジナルディスク識別子を表し、Scは、オリジナルディスクが合法的にコピーされうるディスクのディスク識別子を表し、Spは、再生しようとしているディスクのディスク識別子を表す。Spは、Sd, Scの値を採ることができる。その場合、オリジナルディスクおよびその合法的コピーがそれぞれ再生されているようにしていることになる。

【0064】 K_A および K_{A-1} は、コンテンツ供給者のデジタル署名のためのキー対である。 K_A および K_{A-1} は、例えば、コピーはオリジナルからのみ可能で、オリジナルのコピーからは不可能とすることを保証するCGMSスキームを実現するために必要なデジタル署名のためのキー対である。

【0065】図8および図12において、コンテンツ供給者が、バックアップコピーの作成も含めてオリジナルディスクからのあらゆる複製を禁止することを望む場合、ステップs30で、CCFフラグをネバーコピーにセットする。ステップs31では、キー対発生モジュール21は、第1の例について上述したキー対 K_A および K_{A-1} を生成する。次に、読み出し装置22がディスク1の読み出し専用部分からSdを読み出し(s32)、ステップs33でCCI生成器23がデジタル署名Sig $K_{A-1}(Sd, A)$ を計算する。この場合のコピー管理情報はSig $K_{A-1}(Sd, A)$ と K_A とからなる。記録モジュール25は、次に、データアーカイブ26からデータを読み出し(s34)、ステップs35で、CCI生成器23からのコピー管理情報とともにデータをディスク1に書き込む。

【0066】図5および図13において、上記データで

符号化されたDVDディスク1がDVDプレーヤ13内に挿入されると、ステップs40で、読み出し装置14がディスク1の読み出し専用部分2からSpを読み出す。読み出し装置14は、また、データ領域3からコピー管理情報、すなわちA、 K_A および $\text{Sig}K_{A-1}(S_d, A)$ を読み出す。CCI検証器15は、そこで、ステップs41において、 S_d 、A、 K_A を用いて $\text{Sig}K_{A-1}(S_d, A)$ を検証する。もし、検証が成功すれば、制御はステップs42へ移行し、ここで、データが再生される。そうでなければ、制御はステップs43へ進み、ここでデータの再生が阻止される。この例の動作を更に説明するために、以下に検証処理を詳細に説明する。

【0067】ディスクの識別子領域2から読み出されたSpおよびディスクのデータ領域3から読み出されたAを認識することにより、1方向ハッシュ関数Hを用いて関数 c' を計算することができる。すなわち、 $c' = H(m)$ 、ここに $m = (Sp, A)$ である。したがって、 $c' = H(Sp, A)$ となる。

【0068】関数Hは、関数 $c = H(Sp, A)$ を生成するために記録装置20で用いられたものと同じ関数である。この関数は、ディスク1のデータ領域3から読み出された公開キー K_A を用いて、 $\text{Sig}K_{A-1}(S_d, A)$ を復号化することにより得られる。

【0069】もし、 $c = c'$ 、すなわち、 $H(S_d, A) = H(Sp, A)$ ならば、これは、AとSpの両方もが記録時から不変であり、特に、 $Sp = S_d$ 、すなわち、再生しようとするディスク上のシリアル番号と、データが記録されたディスクのシリアル番号とが同じであることを示している。シリアル番号が一意であるとする、このことは、再生しようとしているディスクがオリジナルディスクであり、よって、それに含まれるデータの再生が許可されることを示している。検証が失敗に終われば、再生しようとしているディスクはコピーであると推測され、その再生が阻止される。

【0070】図8および図14において、コンテンツ供給者がオリジナルディスクからのみバックアップコピーの作成する機能を与えたい場合、ステップs50で、コピー管理フィールドをコピーワンスにセットする。ステップs51では、キー対生成モジュール21がキー対 K_A および K_{A-1} とともに K_H および K_{H-1} を生成する。読み出し装置22は、ディスク1の読み出し専用部分から S_d を読み出し(s52)、ステップs53で、デジタル署名 $\text{Sig}K_{A-1}(S_d, A, K_H)$ を計算する。そこで、記録モジュール25はデータアーカイブ26からデータを読み出し(s54)、ステップs55でディスク1に対してデータとともにCCI生成器23からのコピー管理情報を書き込む。このコピー管理情報は、A、 K_A 、 K_H 、 K_{H-1} および $\text{Sig}K_{A-1}(S_d, A, K_H)$ を含む。

【0071】図5および図15において、上記データで符号化されたDVDディスク1がDVDプレーヤ13内に

に挿入されると、ステップs60で、読み出し装置14がディスク1の読み出し専用部分2からSpを読み出す。読み出し装置14はまた、ディスク1のデータ領域からコピー管理情報、すなわち、A、 K_A 、 K_H 、 K_{H-1} および $\text{Sig}K_{A-1}(S_d, A, K_H)$ を読み出す。CCI検証モジュール15は、先に詳述したように、 S_d 、A、 K_H および K_A を用いてデジタル署名 $\text{Sig}K_{A-1}(S_d, A, K_H)$ を検証する。検証が成功であれば、制御はステップs62へ進み、データが再生される。そうでなければ、制御はステップs63へ進み、データの再生が阻止される。

【0072】オリジナルディスクのバックアップコピーの作成は許容されるので、図10に示した記録装置30の詳細動作は、図16のフローチャートで示される。図10および図15も参照し、ステップs70およびs71は、再生装置により実行されるようなステップs60およびs61と同じである。もし検証が失敗に終われば、それ以降の処理はステップs72で終了する。検証処理内に K_H を含める目的は、 K_H が偽造されたものではないことを確かめるためである。なぜなら、キー対 K_H および K_{H-1} の両部分が含まれており、よって、オリジナルディスク上で潜在的な侵害者に利用可能だからである。検証手順が成功であれば、ステップs73において、読み出し装置36が書き込み先ディスク35の読み出し専用部分からScを読み出す。CCI生成器33は、Aのコピー管理フィールドをコピーワンスからノーモアコピーへ変更し、これをA'として保存する(s74)。CCI生成器33は、ついで、デジタル署名 $\text{Sig}K_{H-1}(Sc, A')$ を計算し(s75)、ステップs76で、書き込み先ディスク35のデータ領域3に、 S_d 、A、 K_H 、 K_A 、 $\text{Sig}K_{A-1}(S_d, A, K_H)$ 、A'および $\text{Sig}K_{H-1}(Sc, A')$ を書き込む。

【0073】図5および図17において、ノーモアコピーフラグが付されたディスクからデータを再生するには、ステップs80で、読み出し装置14がディスク35の読み出し専用部分2からSpを読み出す。読み出し装置14はまた、そのディスクのデータ領域3からコピー管理情報、すなわち、 S_d 、A、 K_H 、 K_A 、 $\text{Sig}K_{A-1}(S_d, A, K_H)$ 、A'および $\text{Sig}K_{H-1}(Sc, A')$ を読み出す(s81)。CCI検証器15は、ついで、 S_d 、A、 K_H を用いてデジタル署名 $\text{Sig}K_{A-1}(S_d, A, K_H)$ を検証する(s82)。このステップは、検証処理の第2部分で用いたキー K_H 自身が偽造されたものでないことを検証するものである。この検証が失敗すれば、再生は阻止される(ステップs85)。検証が成功であれば、次にステップs83で、CCI検証モジュール15が、Sp、A'および K_H を用いて第2のデジタル署名 $\text{Sig}K_{H-1}(Sc, A')$ の検証を行う。もし、 $Sp = Sc$ ならば、このステップは、コピーされたディスク自体がコピーされたものではないことを示し、よって、第2世代コピーの再生を阻止する。検証が成功であれば、再生装置17はデータを再生し

(s84)、そうでなければ再生は阻止される(s85)。

【0074】本発明による方法は、記憶媒体に対して一意なまたはほぼ一意な識別子を関連づけることができる任意の汎用デジタル記録システムに利用することができることが理解されよう。この記憶媒体には、例えば、識別子の不可変記憶のためのROM領域部分を有するスマートカードRAMメモリを含む。

【0075】また、公開鍵アルゴリズムに基づく方法について詳細に説明したが、デジタル署名を行うたの手段を排除するものではない。

【図面の簡単な説明】

【図1】 本発明によるDVDディスクの概略図である。

【図2】 図1のディスクを製造するために使用される装置の概略ブロック図である。

【図3】 コピー防止されたディスクを作成するためにコンテンツ供給者により使用されるべき記録装置の一例を示す概略ブロック図である。

【図4】 図3の記録装置の動作を示すフロー図である。

【図5】 本発明によるDVDプレーヤの概略ブロック図である。

【図6】 図5のプレーヤの動作を示すフロー図である。

【図7】 コピー管理情報の所定の例に基づく、図3の記録装置および図5のプレーヤの詳細な動作を示すフロー図である。

【図8】 本発明の他の例によるコンテンツ供給者により使用されるべき記録装置の概略ブロック図である。

【図9】 図8の記録装置の動作を示すフロー図である。

【図10】 消費者装置に利用されるべき本発明によるデータ記録装置の概略ブロック図である。

【図11】 図10の記録装置の動作を示すフロー図である。

【図12】 オリジナルディスクのコピーが許されない場合の、図8の記録装置の詳細動作を示すフロー図である。

【図13】 再生しようとしているディスクが図12に示した記録動作に従って記録されている場合の図5のプレーヤの詳細動作を示すフロー図である。

【図14】 オリジナルディスクからの1回のコピー生成が許される場合の、図8の記録装置の詳細動作を示すフロー図である。

【図15】 再生しようとしているディスクが図14の記録動作に従って記録されている場合の、図5のプレーヤの詳細動作を示すフロー図である。

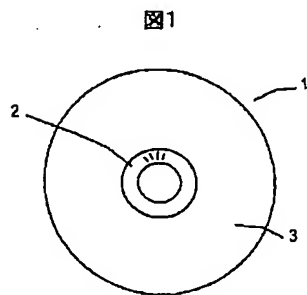
【図16】 記録中のデータ自体が図14の記録動作に従って記録されていた場合の図10の記録装置の詳細動作を示すフロー図である。

【図17】 再生しようとしているディスクが図16に示した記録動作に従って記録されている場合の、図5のプレーヤの詳細動作を示すフロー図である。

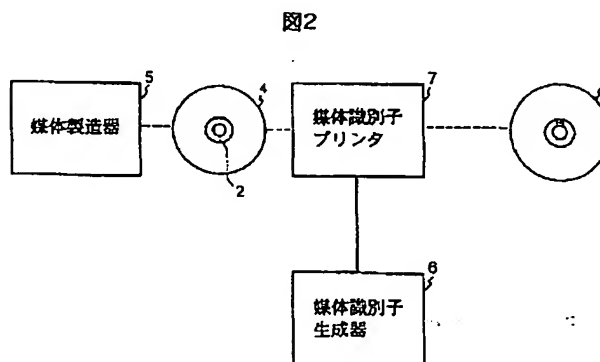
【符号の説明】

- 1 DVDディスク
- 2 識別子領域
- 3 データ領域
- 4 未記録(ブランク)DVDディスク

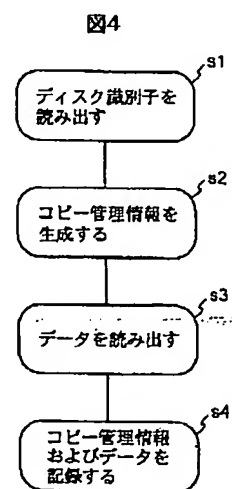
【図1】



【図2】

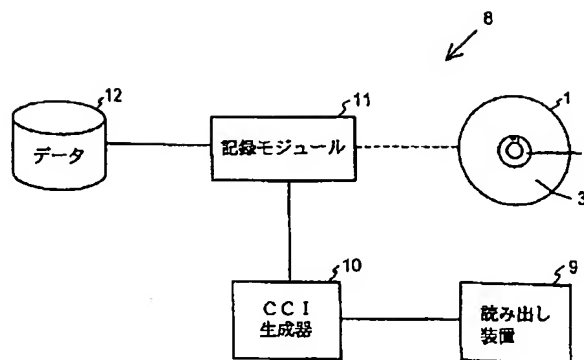


【図4】



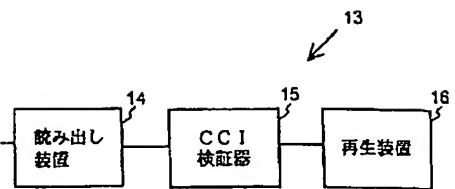
【図3】

図3



【図5】

図5

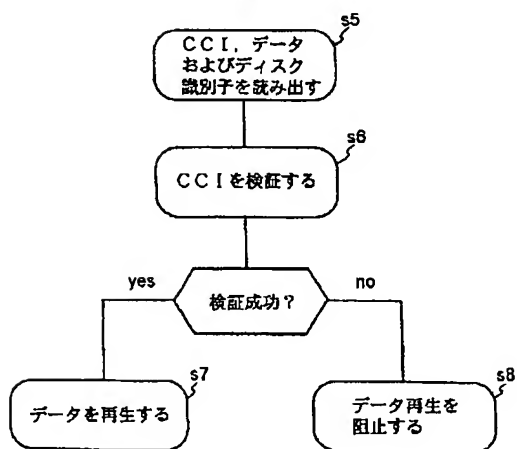


【図9】

図9

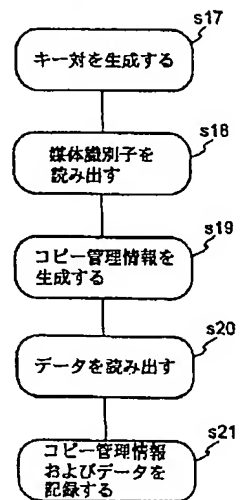
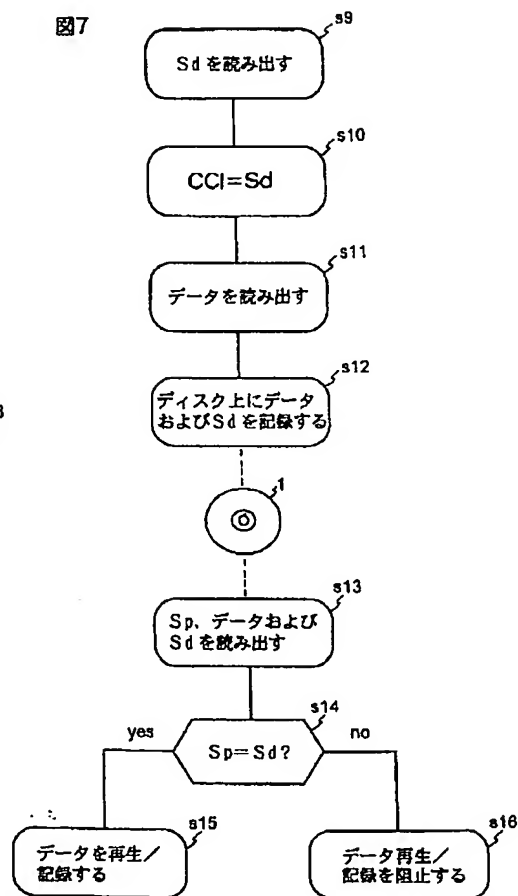
【図6】

図6

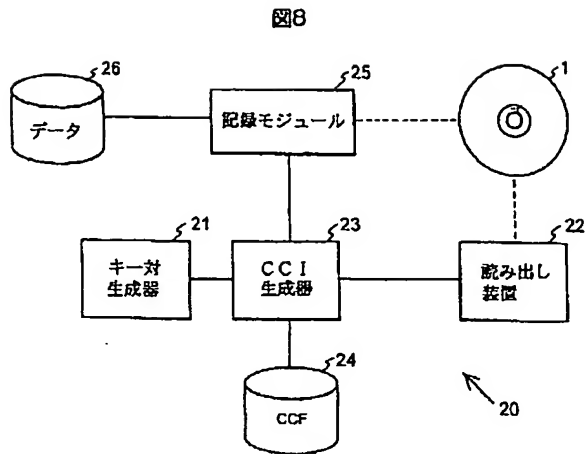


【図7】

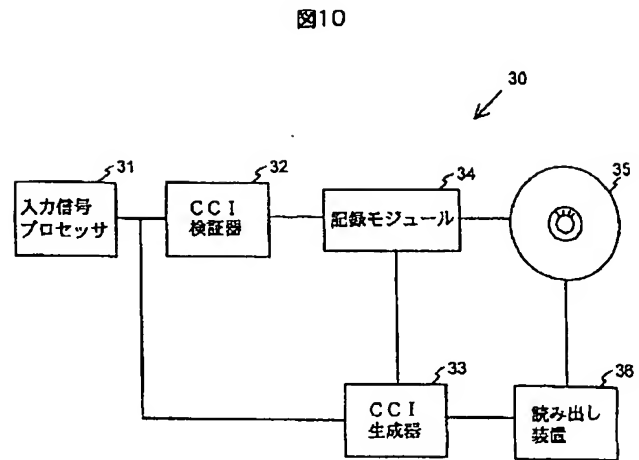
図7



【図8】

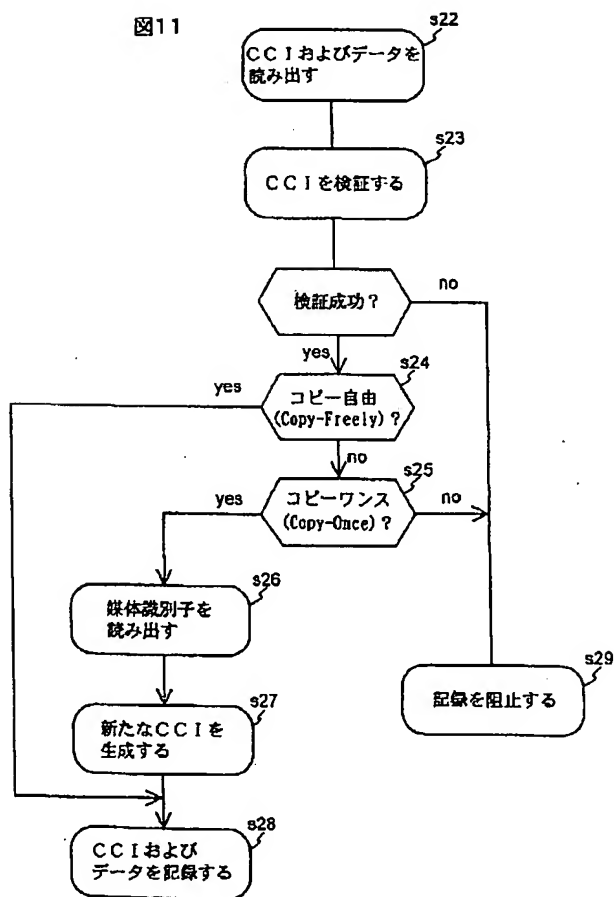


【図10】



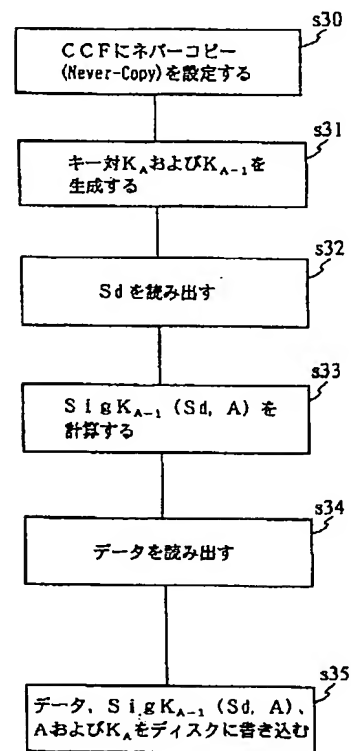
【図11】

図11



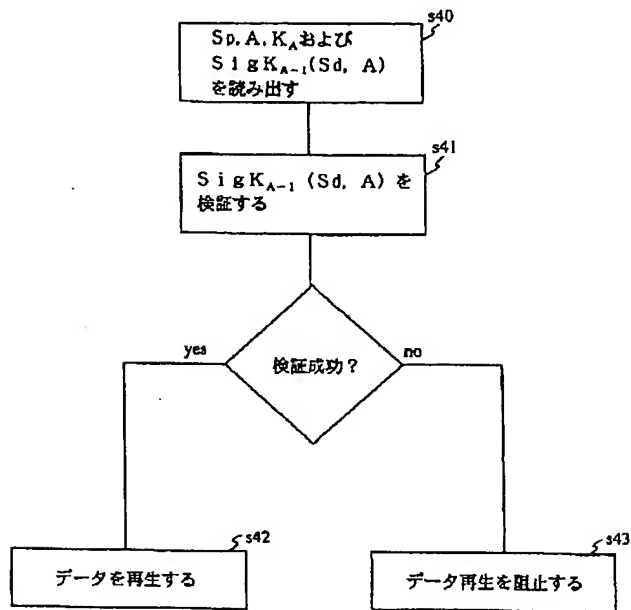
【図12】

図12



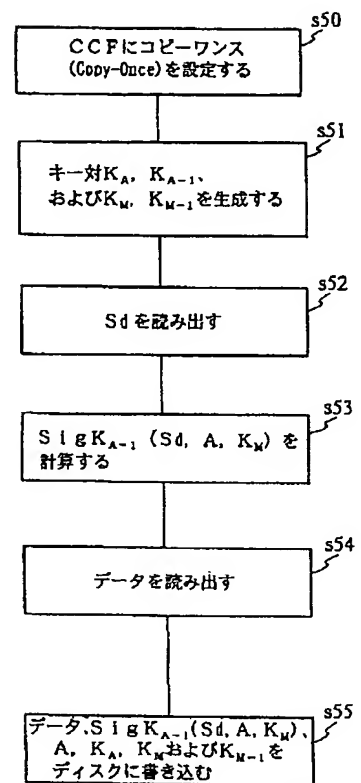
【図13】

図13



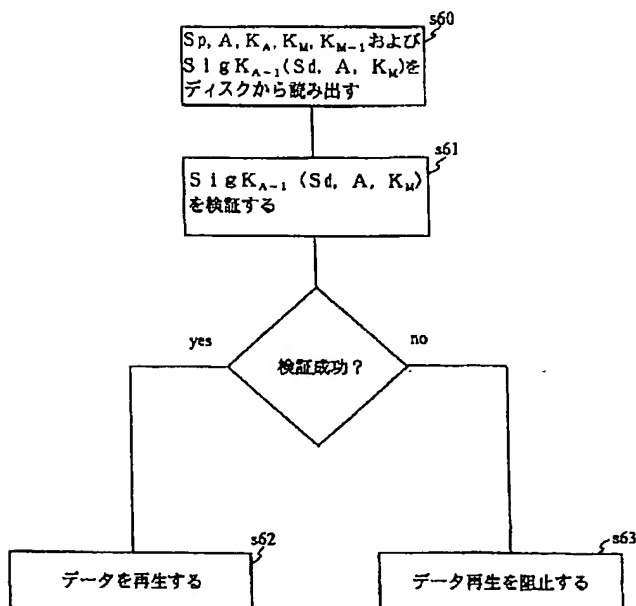
【図14】

図14

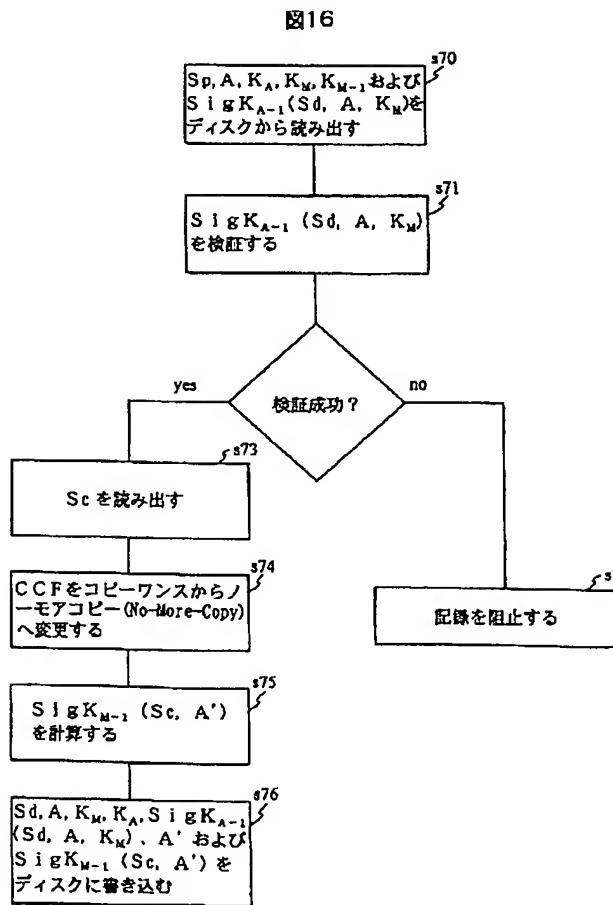


【図15】

図15



【図16】



【図17】

